



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/540,501	06/23/2005	Patrice Hameau	HAMEAU2	2706
1444	7590	11/30/2006	EXAMINER	
BROWDY AND NEIMARK, P.L.L.C.			CHEN, SHIN HON	
624 NINTH STREET, NW			ART UNIT	PAPER NUMBER
SUITE 300				2131
WASHINGTON, DC 20001-5303				

DATE MAILED: 11/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/540,501	HAMEAU ET AL.
	Examiner Shin-Hon Chen	Art Unit 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 23 June 2005.

2a) This action is FINAL. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-21 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-21 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)

2) Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 6/23/05.

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.

5) Notice of Informal Patent Application

6) Other: _____.

DETAILED ACTION

1. Claims 1-21 have been examined.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

3. Claims 1-21 are rejected under 35 U.S.C. 102(e) as being clearly anticipated by Collberg et al. U.S. Pat. No. 6668325 (hereinafter Collberg).

4. As per claim 1, Collberg discloses a method for securing computer systems comprising at least one code interpretation module and memory capacities for storing the interpreted code having measurable physical imprints, said method with the purpose of making attacks based on physical measurements or requiring synchronization with the aforesaid interpreted code, more difficult, consisting of introducing alternatives for executing the interpreted code, said alternatives having an effect on the execution times of the interpreted code or on its measurable physical imprint (Collberg: column 2 lines 10-21).

5. As per claim 2, Collberg discloses the method according to claim 1. Collberg further discloses the method comprising bypasses towards new code portions, so-called "bypass codes",

which do not belong to the original code (Collberg: column 2 lines 58-64).

6. As per claim 3, Collberg discloses the method according to claim 1. Collberg further discloses the method comprising a plurality of implementations of certain instructions, each requiring a different execution time or having a different physical imprint while providing an identical result (Collberg: column 2 lines 64-67).

7. As per claim 4, Collberg discloses the method according to claim 2. Collberg further discloses the method comprising a first mode for introducing "bypass codes" consisting of introducing one or more instructions specific to certain particular locations of the code, either manually or automatically during the generation of the aforesaid code (Collberg: column 3 lines 5-16).

8. As per claim 5, Collberg discloses the method according to claim 4. Granger further discloses wherein the bypass instructions are associated with security levels which correspond to complexity levels of their bypass code, the most complex being considered as the most defensive with regard to security attacks requiring synchronization with the code or measurement of its physical imprint (Collberg: column 2 lines 26-39).

9. As per claim 6, Collberg discloses the method according to claim 2. Collberg further discloses the method comprising a second mode for introducing "bypass codes" consisting of introducing the bypass code in the implementation of the interpreter itself (Collberg: column 15

lines 19-42).

10. As per claim 7, Collberg discloses the method according to claim 6. Collberg further discloses wherein the bypass code introduced into the implementation of the interpreter is executed either systematically by the interpreter or selectively or randomly (Collberg: column 2 lines 22-39).

11. As per claim 8, Collberg discloses the method according to claim 2. Collberg further discloses the method comprising a first mode for realizing "bypass codes" consisting of performing a so-called "superfluous" calculation depending on data known at execution (Collberg: column 18 lines 54-57).

12. As per claim 9, Collberg discloses the method according to claim 2. Collberg further discloses the method comprising a second mode for realizing "bypass codes" consisting of providing the aforesaid first mode with a random draw of an extra datum during the execution of the superfluous calculation, said extra datum being used in the calculation performed by the bypass code (Collberg: column 15 lines 32-35).

13. As per claim 10, Collberg discloses the method according to claim 8. Collberg further discloses wherein the aforesaid first mode for realizing "bypass codes" is improved by attaching different security levels to the implementations of instructions and associating them with all the more complex implementations (Collberg: column 10 lines 65-67: select required level of

obfuscation).

14. As per claim 11, Collberg discloses the method according to claim 2. Collberg further discloses the method comprising a third mode for realizing "bypass codes" consisting of replacing in the aforesaid first and second modes the test for deciding on the next action by a branching in an indirection table containing the addresses of possible actions at an index calculated from variable items (dynamical datum and/or result from a random draw) (Collberg: column 15 lines 26-43).

15. As per claim 12, Collberg discloses the method according to claim 2. Collberg further discloses the method comprising a fourth mode for realizing "bypass codes" consisting of performing a superfluous calculation having the external characteristics of a particular sensitive calculation (Collberg: column 12 lines 34-35 and column 18 lines 54-57).

16. As per claim 13, Collberg discloses the method according to claim 3. Collberg further discloses the method comprising a first mode for introducing a plurality of implementations of certain instructions consisting of enriching the set of instructions recognized by the interpreter with a plurality of implementations for a given instruction (Collberg: column 18 lines 15-39); the aforesaid instructions are performed either manually by programming or automatically upon code generation (Collberg: column 18 lines 15-39).

17. As per claim 14, Collberg discloses the method according to claim 3. Collberg further discloses the method comprising a second mode for introducing the aforesaid plurality of implementations of certain instructions consisting of comprising in the actual implementation of the instruction, a branching to a portion of at least one alternative code with a variable physical imprint or duration, which dynamically determines the implementation to be executed (Collberg: column 27 lines 20-33).

18. As per claim 15, Collberg discloses the method according to claim 14. Collberg further discloses the method comprising a first mode for realizing the aforesaid alternative code consisting of proposing a plurality of different implementations of the instruction and by conditioning the choice of the executed version to a dynamical test, i.e., depending on data known at execution (Collberg: column 2 lines 40-57).

19. As per claim 16, Collberg discloses the method according to claim 14. Collberg further discloses the method comprising a second mode for realizing the aforesaid alternative code consisting of improving the aforesaid first mode for realizing "alternative codes" by providing it with a random draw for achieving the test leading to the dynamical choice of the executed version (Collberg: column 15 lines 32-34).

20. As per claim 17, Collberg discloses the method according to claim 14. Collberg further discloses the method comprising a third mode for realizing the aforesaid "alternative code" consisting of improving the aforesaid first and second modes for realizing "alternative codes"

consisting of replacing the test for deciding on the selected version with a branching in an indirection table containing the addresses of the available version at an index calculated for variable items (Collberg: column 18 lines 15-27).

21. As per claim 18, Collberg discloses the method according to claim 1. Collberg further discloses the method being implemented on a module for interpreting software code, a so-called virtual machine (Collberg: column 18 lines 16-27).

22. As per claim 19, Collberg discloses the method according to claim 18. Collberg further discloses wherein said virtual machine is a Java platform (Collberg: column 18 lines 16-27).

23. As per claim 20, Collberg discloses the method according to claim 1. Collberg further discloses the method being implemented on a module for interpreting physical code (Collberg: column 15 lines 19-43).

24. As per claim 21, Collberg discloses the method according to claim 1. Collberg further discloses the method being implemented on an embedded system and on an interpretation module of the microcontroller or microprocessor type (Collberg: column 4 line 60 – column 5 line 24).

Conclusion

25. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Cronce et al. U.S. Pub. No. 20030236986 discloses protecting software from unauthorized use by converting source code modules to byte codes.

Naumovich et al. U.S. Pub. No. 20040103404 discloses class coalescence for obfuscation of object-oriented software.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shin-Hon Chen
Examiner
Art Unit 2131

SC


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100